

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-91301  
(P2002-91301A)

(43) 公開日 平成14年3月27日 (2002.3.27)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	データシート <sup>*</sup> (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D

審査請求 未請求 請求項の数 9 O L (全 19 頁)

(21) 出願番号 特願2000-284051 (P2000-284051)

(22) 出願日 平成12年9月19日 (2000.9.19)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ  
東京都江東区豊洲三丁目3番3号

(72) 発明者 佐藤 秀紀

東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

(74) 代理人 100064908

弁理士 志賀 正武 (外2名)

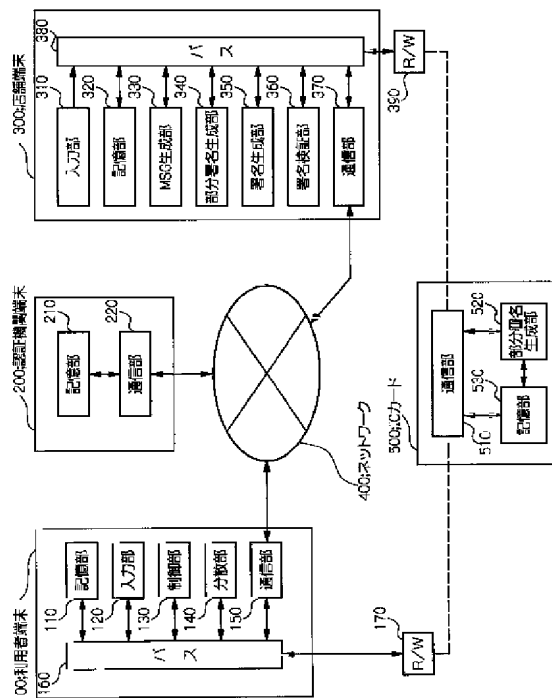
Fターム(参考) 5J104 AA09 AA16 EA04 EA13 JA21  
LA03 LA06 MA02 NA02 PA10

(54) 【発明の名称】 鍵情報分散装置、演算装置および署名検証装置

(57) 【要約】

【課題】 秘密鍵の紛失、盗難などが発生しても鍵情報の機密性の向上を図ることができる鍵情報分散端末、I Cカードおよび店舗端末を提供する。

【解決手段】 電子署名を生成するための鍵情報を $n$ 個 ( $n$ は2以上の自然数) に分割し、分割した鍵情報を $k$ 個 ( $k$ は $1 < k \leq n$ となる自然数) 集めた場合に前記電子署名を生成するための部分鍵情報を生成する分散手段と、所定のプログラムに基づいて電子署名を生成する演算装置に対し、前記分散手段によって生成される部分鍵情報のうち、 $k$ 個未満の部分鍵情報を格納する制御または、他の部分鍵情報のうち $k$ 個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段とを有することを特徴とする。



【特許請求の範囲】

【請求項1】 電子署名を生成するための鍵情報を  $n$  個 ( $n$  は2以上の自然数) に分割し、分割した鍵情報を  $k$  個 ( $k$  は  $1 < k \leq n$  となる自然数) 集めた場合に前記電子署名を生成するための部分鍵情報を生成する分散手段と、  
所定のプログラムに基づいて電子署名を生成する演算装置に対し、前記分散手段によって生成される部分鍵情報のうち、 $k$  個未満の部分鍵情報を格納する制御または、他の部分鍵情報のうち  $k$  個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段と、  
を有することを特徴とする鍵情報分散装置。

【請求項2】 前記電子署名を生成するための鍵情報を  $n$  個 ( $n$  は2以上の自然数) に分割し、分割した鍵情報を  $k$  個 ( $k$  は  $1 < k \leq n$  となる自然数) 集めた場合に前記電子署名が生成される第1の部分鍵情報を生成する第1の分散手段と、  
前記第1の分散手段が生成する第1の部分鍵情報のうち少なくとも1個の第1の鍵情報をさらに  $m$  個 ( $m$  は2以上の自然数) に分割し、分割した鍵情報を  $j$  個 ( $1 < j \leq m$ ) 集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報を生成する第2の分散手段と、  
前記第2の分散手段によって生成される第2の部分鍵情報のうち  $j$  個未満の第2の部分鍵情報と前記第1の分散手段によって生成される第1の部分鍵情報のうち ( $k-1$ ) 個の第1の部分鍵情報を電子署名を生成する演算装置に格納する制御または、  
他の第2の部分鍵情報のうち、 $j$  個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段と、  
を有することを特徴とする鍵情報分散装置。

【請求項3】 電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、  
前記電子署名を生成するための鍵情報が  $n$  個 ( $n$  は2以上の自然数) に分割され、分割された鍵情報を  $k$  個 ( $k$  は  $1 < k \leq n$  となる自然数) 集めた場合に前記電子署名を生成するための部分鍵情報のうち  $k$  個未満の部分鍵情報を記憶する第1の記憶手段と、  
前記署名検証装置から前記通信手段を介して送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第2の記憶手段と、  
前記第1の記憶手段に記憶される部分鍵情報と前記第2の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、  
前記通信手段によって前記部分署名生成手段によって生成される部分署名情報を前記署名検証装置に送信することを特徴とする演算装置。

【請求項4】 電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、  
前記電子署名を生成するための鍵情報が  $n$  個 ( $n$  は2以上の自然数) に分割され、分割された鍵情報を  $k$  個 ( $k$  は  $1 < k \leq n$  となる自然数) 集めた場合に前記電子署名が生成される第1の部分鍵情報のうち  $k$  個未満を記憶する第1の記憶手段と、  
第1の部分鍵情報のうち少なくとも1個の第1の鍵情報がさらに  $m$  個 ( $m$  は2以上の自然数) に分割され、分割された鍵情報を  $j$  個 ( $1 < j \leq m$ ) 集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報のうち  $j$  個未満を記憶する第2の記憶手段と、  
前記署名検証装置から送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第3の記憶手段と、  
前記第2の記憶手段に記憶される第2の部分鍵情報と前記第3の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する第1の部分署名情報と合成することによって第2の部分署名情報が生成される情報となる部分署名情報を生成する部分署名生成手段と、  
前記署名検証装置から送信される第2の部分署名情報と前記第1の記憶手段に記憶される第1の部分鍵情報とに基づいて、前記電子署名によって署名を行うための電子署名を生成する署名情報生成手段とを有し、  
前記通信手段は、前記署名生成手段が生成する電子署名を前記署名検証装置に送信することを特徴とする演算装置。

【請求項5】 演算装置から送信される電子署名によって署名を行うための情報の通信を行い、電子署名を生成する署名検証装置において、  
前記電子署名を生成するための鍵情報が  $n$  個 ( $n$  は2以上の自然数) に分割され、分割された鍵情報を  $k$  個 ( $k$  は  $1 < k \leq n$  となる自然数) 集めた場合に前記電子署名が生成される部分鍵情報を記憶する第1の記憶手段と、  
前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成手段と、  
前記MSG生成手段によって生成されるメッセージを記憶する第2の記憶手段と、  
前記第1の記憶手段に記憶される部分鍵情報と前記第2の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段と、  
前記演算装置から送信される部分署名情報と前記部分署名生成手段によって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成手段と、  
を有することを特徴とする署名検証装置。

【請求項6】 所定のプログラムにより電子署名を生成する演算装置へ電子署名によって署名を行うための情報を送信し、前記演算装置から電子署名を受信する署名検証

証装置において、

前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される第1の部分鍵情報のうち少なくとも1個の第1の鍵情報がさらに $m$ 個( $m$ は2以上の自然数)に分割され、分割された鍵情報を $j$ 個( $1 < j \leq m$ )集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報のうち $j$ 個未満の第2の部分鍵情報を記憶する第1の記憶手段と、

前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成手段と、

前記MSG生成手段によって生成されるメッセージを記憶する第2の記憶手段と、

前記第1の記憶手段に記憶される第2の部分鍵情報と前記第2の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算装置に記憶される第1の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成手段と、を有することを特徴とする署名検証装置。

【請求項7】 電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、前記電子署名によって署名を行う店舗を特定するための情報となる使用先コードと前記電子署名を生成するための部分鍵情報とを記憶する記憶手段と、前記記憶手段に記憶される使用先コードを前記通信手段によって受信する電子署名を行う文書の内容に関する情報となるメッセージに付加するとともに、前記使用先コードが付加されたメッセージと前記記憶手段に記憶される部分鍵情報とに基づいて、前記署名検証装置によって生成される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、前記通信手段は、前記部分署名生成手段が生成する部分署名を前記署名検証装置に送信することを特徴とする演算装置。

【請求項8】 演算装置から送信される署名を行うための情報に基づいて、電子署名を生成する電子署名生成プログラムを記憶したコンピュータ読みとり可能な記録媒体において、

前記電子署名生成プログラムは、

前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される部分鍵情報を記憶する記憶ステップと、

前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成ステップと、

前記MSG生成ステップにおいて生成されるメッセージと、前記記憶ステップにおいて記憶される部分鍵情報と

に基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成ステップと、

前記演算装置から送信される部分署名情報と前記部分署名生成ステップによって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成ステップと、をコンピュータに行わせることを特徴とする電子署名生成プログラムを記録した記録媒体。

【請求項9】 所定のプログラムにより電子署名を生成する演算装置へ署名を行うための情報を送信し、前記演算装置から電子署名を受信する電子署名プログラムを記憶したコンピュータ読みとり可能な記録媒体において、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される第1の部分鍵情報のうち少なくとも1個の第1の鍵情報をさらに $m$ 個( $m$ は2以上の自然数)に分割され、分割された鍵情報を $j$ 個( $1 < j \leq m$ )集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報のうち $j$ 個未満の第2の部分鍵情報を記憶する記憶ステップと、

前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成ステップと、

前記記憶ステップにおいて記憶される第2の部分鍵情報と前記MSG生成ステップにおいて生成されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算装置に記憶される第1の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成ステップと、

をコンピュータに行わせることを特徴とする電子署名プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子署名を生成するための秘密鍵の機密性を向上することができる鍵情報分散端末、ICカードおよび店舗端末に関するものである。

【0002】

【従来の技術】近年、印章の代わりに、ICチップを搭載した記録媒体(以下、ICカード)に署名用秘密鍵を書き込み、利用者は、このICカードを携帯し、店等における商品の購入や契約時において、この秘密鍵を使用して電子署名を生成し、契約を成立させることが行われつつある。このICカードの紛失、盗難が発生すると、悪意ある第三者に不正使用されるといった危険性がある。この危険を防止するために、以下に示す方法があった。

① ICカードにPIN(個人識別番号)を設定する方法

パスワードや4桁の暗証番号であるPINをICカードに設定し、このPINを入力すると、ICカードに設定されている秘密鍵によって署名を行うことができるものである。

②CRL(鍵廃棄リスト)を用いる方法。

ICカードに設定された秘密鍵は、秘密鍵を利用する利用者の身分を証明するための証明書があり、この証明書は、認証機関によって管理されている。ICカードの利用者は、ICカードを紛失した場合にこの認証機関に連絡し、秘密鍵を無効にする届け出を行う。これにより、秘密鍵が無効になり、ICカードの不正使用を防ぐことができる。

【0003】

【発明が解決しようとする課題】しかしながら、上述した従来の方法においては、以下のような問題点があった。すなわち、①の方法においては、ICカードの物理的なセキュリティが破られると、秘密鍵が読み出され、不正使用される可能性があった。さらに、ICカードの使用毎にPINの入力をする必要があるため、カード使用者およびカード取り扱い店にとって手間がかかっていた。一方、②の方法においては、カード使用者がカードの紛失に気づいてから、ICカードの秘密鍵を無効にする手続きを行うこととなるために、実際にカードを紛失してから利用者がカードの紛失に気づくまでの間と秘密鍵を無効にする手続きが完了するまでの間とがあるため、この間に悪意ある第三者に不正使用される可能性があった。さらに、②の方法においては、使用者の届け出によって秘密鍵を無効にした場合、ICカードを使用するには、新たに認証機関に秘密鍵を使用するための手続きを行う必要があり、カード使用者にとってこの手続きが煩雑であった。

【0004】本発明はこのような事情に鑑みてなされたもので、その目的は、秘密鍵の紛失、盗難などが発生しても鍵情報の機密性の向上を図ることができる鍵情報分散端末、ICカードおよび店舗端末を提供することにある。

【0005】

【課題を解決するための手段】上記目的を達成するために、本発明は、電子署名を生成するための鍵情報を $n$ 個( $n$ は2以上の自然数)に分割し、分割した鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名を生成するための部分鍵情報を生成する分散手段と、所定のプログラムに基づいて電子署名を生成する演算装置に対し、前記分散手段によって生成される部分鍵情報のうち、 $k$ 個未満の部分鍵情報を格納する制御または、他の部分鍵情報のうち $k$ 個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段とを有することを特徴とする。

【0006】また、本発明は、前記電子署名を生成する

ための鍵情報を $n$ 個( $n$ は2以上の自然数)に分割し、分割した鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される第1の部分鍵情報を生成する第1の分散手段と、前記第1の分散手段が生成する第1の部分鍵情報のうち少なくとも1個の第1の鍵情報をさらに $m$ 個( $m$ は2以上の自然数)に分割し、分割した鍵情報を $j$ 個( $1 < j \leq m$ )集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報を生成する第2の分散手段と、前記第2の分散手段によって生成される第2の部分鍵情報のうち $j$ 個未満の第2の部分鍵情報と前記第1の分散手段によって生成される第1の部分鍵情報のうち( $k-1$ )個の第1の部分鍵情報を電子署名を生成する演算装置に格納する制御または、他の第2の部分鍵情報のうち、 $j$ 個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段とを有することを特徴とする。

【0007】また、本発明は、電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名を生成するための部分鍵情報のうち $k$ 個未満の部分鍵情報を記憶する第1の記憶手段と、前記署名検証装置から前記通信手段を介して送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第2の記憶手段と、前記第1の記憶手段に記憶される部分鍵情報と前記第2の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、前記通信手段によって前記部分署名生成手段によって生成される部分署名情報を前記署名検証装置に送信することを特徴とする。

【0008】また、本発明は、電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される第1の部分鍵情報のうち $k$ 個未満を記憶する第1の記憶手段と、第1の部分鍵情報のうち少なくとも1個の第1の鍵情報がさらに $m$ 個( $m$ は2以上の自然数)に分割され、分割された鍵情報を $j$ 個( $1 < j \leq m$ )集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報のうち $j$ 個未満を記憶する第2の記憶手段と、前記署名検証装置から送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第3の記憶手段と、前記第2の記憶手段に記憶される第2の部分鍵情報と前記第3の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する第1の部

分署名情報と合成することによって第2の部分署名情報が生成される情報となる部分署名情報を生成する部分署名生成手段と、前記署名検証装置から送信される第2の部分署名情報と前記第1の記憶手段に記憶される第1の部分鍵情報とに基づいて、前記電子署名によって署名を行うための電子署名を生成する署名情報生成手段とを有し、前記通信手段は、前記署名生成手段が生成する電子署名を前記署名検証装置に送信することを特徴とする。

【0009】また、本発明は、演算装置から送信される電子署名によって署名を行うための情報の通信を行い、電子署名を生成する署名検証装置において、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される部分鍵情報を記憶する第1の記憶手段と、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成手段と、前記MSG生成手段によって生成されるメッセージを記憶する第2の記憶手段と、前記第1の記憶手段に記憶される部分鍵情報と前記第2の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段と、前記演算装置から送信される部分署名情報と前記部分署名生成手段によって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成手段とを有することを特徴とする。

【0010】また、本発明は、所定のプログラムにより電子署名を生成する演算装置へ電子署名によって署名を行うための情報を送信し、前記演算装置から電子署名を受信する署名検証装置において、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される第1の部分鍵情報のうち少なくとも1個の第1の鍵情報がさらに $m$ 個( $m$ は2以上の自然数)に分割され、分割された鍵情報を $j$ 個( $1 < j \leq m$ )集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報のうち $j$ 個未満の第2の部分鍵情報を記憶する第1の記憶手段と、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成手段と、前記MSG生成手段によって生成されるメッセージを記憶する第2の記憶手段と、前記第1の記憶手段に記憶される第2の部分鍵情報と前記第2の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算装置に記憶される第1の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成手段とを有することを特徴とする。

【0011】また、本発明は、電子署名を生成する署名検証装置に接続される通信手段を有する演算装置におい

て、前記電子署名によって署名を行う店舗を特定するための情報となる使用先コードと前記電子署名を生成するための部分鍵情報とを記憶する記憶手段と、前記記憶手段に記憶される使用先コードを前記通信手段によって受信する電子署名を行う文書の内容に関する情報となるメッセージに付加するとともに、前記使用先コードが付加されたメッセージと前記記憶手段に記憶される部分鍵情報とに基づいて、前記署名検証装置によって生成される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、前記通信手段は、前記部分署名生成手段が生成する部分署名を前記署名検証装置に送信することを特徴とする。

【0012】また、本発明は、演算装置から送信される署名を行うための情報に基づいて、電子署名を生成する電子署名生成プログラムを記憶したコンピュータ読みとり可能な記録媒体において、前記電子署名生成プログラムは、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される部分鍵情報を記憶する記憶ステップと、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成ステップと、前記MSG生成ステップにおいて生成されるメッセージと、前記記憶ステップにおいて記憶される部分鍵情報とに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成ステップと、前記演算装置から送信される部分署名情報と前記部分署名生成ステップによって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成ステップとをコンピュータに行わせることを特徴とする。

【0013】また、本発明は、所定のプログラムにより電子署名を生成する演算装置へ署名を行うための情報を送信し、前記演算装置から電子署名を受信する電子署名プログラムを記憶したコンピュータ読みとり可能な記録媒体において、前記電子署名を生成するための鍵情報が $n$ 個( $n$ は2以上の自然数)に分割され、分割された鍵情報を $k$ 個( $k$ は $1 < k \leq n$ となる自然数)集めた場合に前記電子署名が生成される第1の部分鍵情報のうち少なくとも1個の第1の鍵情報がさらに $m$ 個( $m$ は2以上の自然数)に分割され、分割された鍵情報を $j$ 個( $1 < j \leq m$ )集めた場合に前記第1の部分鍵情報が生成される第2の部分鍵情報のうち $j$ 個未満の第2の部分鍵情報を記憶する記憶ステップと、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するMSG生成ステップと、前記記憶ステップにおいて記憶される第2の部分鍵情報と前記MSG生成ステップにおいて生成されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算

装置に記憶される第1の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成ステップとをコンピュータに行わせることを特徴とする。

【0014】

【発明の実施の形態】以下、本発明の一実施形態による鍵情報分散端末、ICカードおよび店舗端末を図面を参照して説明する。ここでは、ICカードを所有する利用者が、店舗に出向き、電子署名によって取引の契約を行う場合を例として説明する。図1は、この発明の一実施形態による電子署名システムの構成を示す概略ブロック図である。この図において、電子署名システムは、利用者端末100と、認証機関端末200と、店舗端末300と、ネットワーク400と、ICカード500とによって構成される。

【0015】利用者端末100は、記憶部110と、入力部120と、分散部140と、通信部150とがバス160によって接続され、装置各部間で各種データがバス160を介して制御部130の制御に基づいて送受信される。この利用者端末100は、例えば、利用者の自宅に設けられる。

【0016】制御部130は、分散部140に対し、秘密鍵SKを所定の閾値kで $n+1$ 個に分散する制御を行うとともに、バス160を介して各部のデータの転送を行う。ここで、秘密鍵SKの分散について説明する。この秘密鍵SKの分散は、シークレットシェアによって行われる。ここでいうシークレットシェアは、図2に示すように、秘密鍵SKは、しきい値kでn個の部分秘密鍵SK1～SKnに分散される。そして、分散された部分秘密鍵SK1～SKnとメッセージとに基づいて、部分署名S1～Snが生成される。そして、部分署名S1～Snのうち、任意の部分署名Snがk個集まった場合に、署名Sが生成される。

【0017】次に、図1に戻り、分散部140は、制御部130の指示に基づき、秘密鍵SKを設定されるしきい値k(=2)で $(n+1)$ 個の部分秘密鍵を生成する。分散部140によって生成される部分秘密鍵は、1個の部分秘密鍵SKaと、n個の部分秘密鍵SKb1～SKbnとして出力される。記憶部110は、認証機関の公開鍵証明証において証明されている公開鍵PKと秘密鍵SKとの情報を記憶する。また、記憶部110は、分散部140が生成する部分秘密鍵SKa、部分秘密鍵SKb1～SKbnを記憶する。また、記憶部110は、各種データを記憶する。

【0018】通信部150は、ネットワーク400を介して、認証機関端末200および店舗端末300と通信を行う。入力部120は、利用者端末100を使用する利用者からの入力に応じた信号を出力する。さらに、利用者端末100の外部には、ICカード500とバス160の間のデータの送受信を行う入出力装置(以下、

「R/W」と称す)170が接続される。

【0019】認証機関端末200は、記憶部210と、通信部220とによって構成される。記憶部210は、利用者端末100の利用者が所有する公開鍵PKを記憶する。通信部220は、ネットワーク400を介して利用者端末100または店舗端末300と通信を行い、必要に応じて利用者の公開鍵PKの送受信を行う。この認証機関端末200は、例えば、公開鍵を保管する認証機関に設けられる。

【0020】店舗端末300は、入力部310と、記憶部320と、MSG生成部330と、部分署名生成部340と、署名生成部350と、署名検証部360と、通信部370と、バス380とによって構成される。店舗端末300の各部は、バス380によって接続され、制御部によってデータの送受信が制御される。この店舗端末300は、例えば、商品の販売店や、金融機関などの店舗iに設けられる(ただし、 $1 \leq i \leq n$ であり、nは、使用先となる店舗端末300の数)。

【0021】入力部310は、利用者から入力される指示に応じた信号を出力する。記憶部320は、公開鍵PK、部分秘密鍵SKbiを記憶する。また、記憶部320は、各種データを記憶する。MSG生成部330は、契約者となる利用者と契約を結ぶための契約書となるメッセージ(以下、「Msg」と称す)を生成する。部分署名生成部340は、部分秘密鍵SKbnとMsgとに基づいて、部分署名SKnを生成する。署名生成部350は、部分署名Sa～Snがk個集まった場合に契約を成立させるための電子署名となる署名Sを生成する。

【0022】署名検証部360は、署名生成部340が生成した署名Sと公開鍵PKとに基づいて、署名Sが保証できるか否かを検証する。通信部370は、ネットワーク400を介して利用者端末100または認証機関端末200と通信を行う。さらに、店舗端末300の外部には、バス380とICカード500との間のデータの送受信を行うR/W390が接続される。

【0023】次に、図3のフローチャートを用いて、図1の電子署名システムの動作について説明する。まず、利用者は、利用者端末100によって公開鍵PKと秘密鍵SKを生成し、ネットワーク400を介して公開鍵PKを認証機関端末200へ送信して登録するとともに、秘密鍵SKを記憶部110に記憶する。一方、店舗iの店員は、店舗端末300によって、ネットワーク400を介して認証機関200から利用者の公開鍵PKを読み出して、記憶部320に記憶する(ステップS1)。次に、利用者は、入力部120から、秘密鍵SKの分割の指示を入力する。入力部120から秘密鍵SKの分割が指示されると、制御部130は、記憶部110から秘密鍵SKを読み出して分散部140へ出力するとともに、しきい値2で $(n+1)$ 個に分割する指示を行う(ステップS2)。

【0024】分割の指示を受けると、分散部140は、記憶部110から出力された秘密鍵SKをしきい値2で $(n+1)$ 個に分割し、分割結果を部分秘密鍵SKa、部分秘密鍵SKb1～SKbnとして記憶部110に記憶する(ステップS3)。部分秘密鍵SKa、部分秘密鍵SKb1～SKbnが記憶部110に記憶された後、利用者によってICカード500がR/W170に挿入されると、制御部130は、記憶部110に記憶された部分秘密鍵SKaを読み出し、バス160を介してR/W170に出力する。R/W170は、利用者端末100から出力された部分秘密鍵SKaをICカード500に出力する。ICカード500は、通信部510を介してR/W170から部分秘密鍵SKaを受信すると、記憶部530に記憶する(ステップS4)。

【0025】次に、利用者は、ICカードを利用する店舗であって、利用者自身が部分秘密鍵SKb1の管理を信頼できる店舗iを選択し、選択した店舗iの店舗端末300に部分秘密鍵SKbiを送信する指示を入力部120から入力する。入力部120から店舗端末300に部分秘密鍵SKbiを送信する指示が入力されると、制御部130は、バス160と通信部150とネットワーク400を介して店舗端末300の通信部370に部分秘密鍵SKbiを送信する(ステップS5)。通信部370によって利用者端末100から部分秘密鍵SKbiを受信すると、受信した部分秘密鍵SKbiを記憶部320に記憶し、利用者リストに登録する(ステップS6)。

【0026】次に、利用者は、取引の契約を行う場合、ICカード500を携帯して、店舗端末300が設置されている店舗iへ出向く。そして、利用者は、店舗端末300の従業員に、取引の契約を行うための契約書の作成を依頼する。従業員は、契約を行うために必要な情報を入力部310から入力し、Msgの生成を指示する。MSG生成部330は、入力部310から入力された情報に基づいて、Msgを生成し(ステップS8)、生成したMsgを記憶部320に記憶する。

【0027】次に、利用者と従業員との間で取引に関する交渉がなされた後、利用者が取引の契約をする場合、利用者は、ICカード500を店舗端末300のR/W390に挿入する。ICカード500がR/W390に挿入された後、従業員によって入力部310からMsgの転送が指示されると、記憶部320は、記憶しているMsgをR/W390に出力する。R/W390は、店舗端末300から出力されたMsgを挿入されているICカード500の通信部510に転送する(ステップS9)。通信部510は、R/W390から転送されたMsgを記憶部530に出力する。記憶部530は、通信部510から出力されたMsgを記憶する。

【0028】次に、部分署名生成部520は、記憶部530にMsgが記憶されると、記憶されたMsgと部分

秘密鍵SKaとを読み出し、読み出したMsgと部分秘密鍵SKaとに基づいて、部分署名Saを生成する(ステップS10)。そして、部分署名生成部520は、店舗端末300に生成した部分署名生成部Saを通信部510に出力する。通信部510は、部分署名生成部520から出力された部分署名生成部SaをR/W390を介して店舗端末300に転送する(ステップS11)。部分署名生成部Saが送信されると、店舗端末300の記憶部320は、ICカード500から転送された部分署名生成部Saを記憶する(ステップS12)。

【0029】一方、店舗端末300の部分署名生成部340は、ICカードにMsgの転送が完了すると、記憶部320に記憶されているMsgと利用者の部分秘密鍵SKbiとを読み出して、店舗iにおける部分署名Sbiを生成する(ステップS13)。部分署名Sbiが生成されると、署名生成部350は、記憶部320に記憶されている部分署名生成部Saを読み出し、この部分署名生成部Saと部分署名生成部340によって生成された部分署名Sbiとに基づいて、署名Sを生成する(ステップS14)。署名Sが生成されると、署名検証部360は、記憶部320から利用者の公開鍵PKを読み出し、生成された署名Sを検証する(ステップS15)。

【0030】上記の実施形態において、利用者端末100の入力部120から入力される利用者からの指示に応じて店舗端末300に部分秘密鍵SKb1～SKbnのうち部分秘密鍵SKbiを送信するようにしたので、利用者自身が部分秘密鍵SKbnの管理を信頼できる店舗を選択して送信することができる。これにより、いずれかの部分秘密鍵SKb1～SKbnを有していない店舗において、ICカード500を利用することができないので、ICカード500の使用範囲を限定でき、これにより、ICカード500の盗難、部分秘密鍵SKaの情報が盗まれた場合において、部分秘密鍵SKaが第三者に悪用される可能性を低減させることができる効果が得られる。

【0031】次に、この発明の第2の実施形態について、図面を用いて説明する。図4は、第2の実施形態における電子署名システムの構成を示す概略ブロック図である。同図において図1の各部に対応する部分には同一の符号を付け、その説明を省略する。利用者端末100の分散部141は、秘密鍵SKを部分秘密鍵SKaと部分秘密鍵SKbとに分割する。また、分散部141は、部分秘密鍵SKbを制御部130からの指示に基づき、しきい値 $k (=2)$ で $(n+1)$ 個の部分秘密鍵を生成する。分散部141によって生成される部分秘密鍵は、1個の部分秘密鍵SKb0と、 $n$ 個の部分秘密鍵SKb1～SKbnとして出力される。

【0032】店舗端末300の署名生成部351は、部分署名Sbiと部分署名Sb0とに基づいて部分署名Sbを生成し、生成した部分署名SbをICカード500

に送信する指示をする。ICカード500の署名生成部540は、部分署名Sbと部分秘密鍵SKaとに基づいて、署名Sを生成する。

【0033】次に、図4の構成における装置各部の動作について、図5のフローチャートを用いて説明する。まず、図1のステップS1の処理と同様に、利用者端末100によって公開鍵PKが認証機関端末200に登録され、秘密鍵SKが記憶部110に記憶されるとともに、店舗端末300によって、認証機関200から利用者の公開鍵PKが読み出され、記憶部320に記憶される（ステップS51）。

【0034】次に、利用者は、入力部120から、秘密鍵SKの分割の指示を入力する。入力部120から秘密鍵SKの分割が指示されると、制御部130は、記憶部110から秘密鍵SKを読み出して分散部141へ出力するとともに、しきい値2で $(n+1)$ 個に分割する指示を行う。

【0035】分割の指示を受けると、分散部141は、まず、記憶部110から出力された秘密鍵SKを部分秘密鍵SKaと部分秘密鍵SKbとに分割し（ステップS52）、部分秘密鍵SKaを記憶部110に記憶する。次いで、分散部141は、制御部130からの指示に基づき、部分秘密鍵SKbをしきい値2で $(n+1)$ 個に分割し（ステップS53）、分割結果を部分秘密鍵SKb0～SKbnとして記憶部110に記憶する。部分秘密鍵SKa、部分秘密鍵SKb0～SKbnが記憶部110に記憶された後、利用者によってICカード500がR/W170に挿入されると、制御部130は、記憶部110に記憶された部分秘密鍵SKaと部分秘密鍵SKb0とを読み出し、バス160とR/W170を介して、ICカード500に出力する。ICカード500は、通信部510を介してR/W170から部分秘密鍵SKa、部分秘密鍵SKb0を受信すると、記憶部530に記憶する（ステップS54）。

【0036】次に、利用者は、ICカードを利用する店舗であって、利用者自身が部分秘密鍵SKbnの管理を信頼できる店舗iを選択し、選択した店舗iの店舗端末300に部分秘密鍵SKbiを送信する指示を入力部120から入力する。入力部120から店舗端末300に部分秘密鍵SKbiを送信する指示が入力されると、制御部130は、バス160と通信部150とネットワーク400を介して店舗端末300の通信部370に部分秘密鍵SKbiを送信する（ステップS55）。通信部370によって利用者端末100から部分秘密鍵SKbiを受信すると、受信した部分秘密鍵SKbiを記憶部320に記憶し、利用者リストに登録する（ステップS56）。

【0037】次に、利用者は、第1の実施形態と同様に、ICカード500を携帯して、店舗端末300が設置されている店舗iへ出向き、契約書の作成を依頼す

る。従業員は、店舗端末300によって署名対象となるMsgを生成し（ステップS56）、生成したMsgを記憶部320に記憶する。

【0038】次に、利用者と従業員との間で取引に関する交渉がなされた後、利用者が取引の契約をする場合、利用者によってICカード500がR/W390に挿入された後、従業員によって入力部310からMsgの転送が指示されると、記憶部320は、記憶しているMsgをR/W390に出力する。R/W390は、店舗端末300から出力されたMsgを挿入されているICカード500の通信部510に転送する（ステップS59）。通信部510は、R/W390から転送されたMsgを記憶部530に出力する。記憶部530は、通信部510から出力されたMsgを記憶する。

【0039】次に、部分署名生成部520は、記憶部530にMsgが記憶されると、記憶部530から記憶されたMsgと部分秘密鍵SKb0とを読み出し、読み出したMsgと部分秘密鍵SKb0とに基づいて、部分署名Sb0を生成する（ステップS60）。そして、部分署名生成部520は、生成した部分署名生成部Sb0を通信部510に出力する。通信部510は、部分署名生成部520から出力された部分署名生成部SaをR/W390を介して店舗端末300に転送する（ステップS61）。部分署名生成部Saが送信されると、店舗端末300の記憶部320は、ICカード500から転送された部分署名生成部Sb0を記憶する（ステップS62）。

【0040】一方、店舗端末300の部分署名生成部340は、ICカードにMsgの転送が完了した後、記憶部320に記憶されているMsgと利用者の部分秘密鍵SKbiとを読み出して、店舗iにおける部分署名Sbiを生成する（ステップS63）。部分署名Sbiが生成されると、署名生成部351は、記憶部320に記憶されている部分署名生成部Sb0を読み出し、この部分署名生成部Sb0と部分署名生成部340によって生成された部分署名Sbiとに基づいて、部分署名Sbを生成し（ステップS64）、R/W390に対し、生成した部分署名SbをICカード500に送信する指示を行う。

【0041】R/W390は、署名生成部351からの指示を受けて、部分署名SbをICカード500に転送する（ステップS65）。部分署名Sbが転送されると、ICカード500の通信部510は、転送された部分署名Sbを記憶部530に出力し、記憶する。部分署名Sbが記憶部530に記憶されると、署名生成部540は、記憶部530に記憶されている部分署名Sbと秘密鍵SKaとを読み出し、署名Sを生成する（ステップS66）。そして、署名生成部540は、生成した署名Sを記憶部530に記憶した後、通信部510によって店舗端末300に送信する指示を行う。通信部510



は、署名生成部540からの指示を受けて、署名SをR/W390を介して店舗端末300に送信する(ステップS67)。

【0042】店舗端末300の記憶部320は、R/W390を介してICカード500から送信された署名Sを記憶する(ステップS68)。署名Sが記憶された後、署名検証部360は、記憶部320から署名Sと利用者の公開鍵PKを読み出し、公開鍵PKによって署名Sの検証を行う(ステップS69)。

【0043】上述の実施形態においては、秘密鍵SKを部分秘密鍵SKaと部分秘密鍵SKbとに分割した後、部分秘密鍵SKbをさらに、部分秘密鍵SKb0～部分秘密鍵SKbnに分割し、部分秘密鍵SKaと部分秘密鍵SKb0とをICカード500に記憶し、部分秘密鍵SKb1～部分秘密鍵SKbnをそれぞれ店舗に送信するようにした。これにより、店舗同士が結託し、部分秘密鍵SKbnを2つ集めた場合においても、部分秘密鍵SKbしか生成できないすなわち、秘密鍵SKを生成することが不可能であるので、署名Sを生成して不正使用することを防ぐことが可能である。なお、上述の実施形態において、秘密鍵SKを部分秘密鍵SKaと部分秘密鍵SKbとに分割したが、秘密鍵SKをm個(mは2以上の自然数)に分割し、分割した鍵情報をj個( $1 < j \leq m$ )集めた場合に第1の部分鍵情報が生成されるようにしてもよい。

【0044】次に、この発明の第3の実施形態について図面を用いて説明する。図6は、第3の実施形態における電子署名システムの構成を示す概略ブロック図である。この図において、図1の各部に対応する部分には、同一の符号を付け、その説明を省略する。利用者端末100の制御部131は、図1の制御部130の機能にさらに、乱数生成部180に乱数の生成を指示する機能を有し、利用者端末100の各部の動作を制御する。乱数生成部180は、制御部130からの指示に基づいて、乱数を生成する。

【0045】部分秘密鍵演算部190は、部分秘密鍵SKbと乱数Rとf(i)とに基づいて、以下に示す(1)式を用いて部分秘密鍵SKbiを演算する。

$$SKb + H(f(i) \parallel R) \dots\dots (1)$$

ただし、 $H(f(i) \parallel R)$ はハッシュ関数によって計算をおこなうものである。f(i)は、ユニークコードであり、店舗に設置された店舗端末300毎に異なる値が設定される。このユニークコードf(i)は、例えば、利用者によって任意に決定される値であり、例えば、利用者に関する情報、利用する店舗iの店の名前、電話番号、住所などの情報に基づいて決定される。

【0046】ICカード500の部分秘密鍵演算部550は、部分秘密鍵SKaと乱数Rとユニークコードf(i)とに基づいて、以下に示す(2)式を用いて部分秘密鍵SKaiを演算する。

$$SKa - H(f(i) \parallel R) \dots\dots (2)$$

【0047】部分署名生成部520は、Msgと部分秘密鍵SKaiとに基づいて、以下に示す(3)式を用いて部分署名Saを生成する。

$$Sa = MSG^{SKai} \bmod(n) \dots\dots (3)$$

部分署名生成部340は、Msgと部分秘密鍵SKbiとに基づいて、以下に示す(4)式を用いて部分署名Sbを生成する。

$$Sb = MSG^{SKbi} \bmod(n) \dots\dots (4)$$

【0048】署名生成部350は、部分署名Saと部分署名Sbとに基づいて、以下に示す(5)式を用いて、署名Sを生成する。

$$S = Sai \times Sbi \bmod(n) \dots\dots (5)$$

【0049】次に、図6の構成における装置の動作について図7および図8のフローチャートを用いて説明する。図7は、図6の構成における装置の動作を説明するフローチャート、図8は、部分秘密鍵SKa、部分秘密鍵SKbiをICカード500、店舗端末300に設定する動作を説明するためのフローチャートである。

【0050】まず、図7のフローチャートを用いて図6の構成における装置の動作について説明する。利用者端末100によって公開鍵PKが認証機関端末200に登録され、秘密鍵SKが記憶部110に記憶されるとともに、店舗端末300によって、認証機関200から利用者の公開鍵PKが読み出され、記憶部320に記憶される。

【0051】次に、利用者は、入力部120から、ユニークコードf(i)を入力するとともに、秘密鍵SKの分割の指示を入力する。入力部120から秘密鍵SKの分割が指示されると、制御部131は、ユニークコードf(i)を記憶部110に記憶するとともに、秘密鍵SKを分割し、分割した部分秘密鍵をICカード500と、店舗端末300に設定する制御を行う(ステップS101)。ここで、ステップS101における装置の動作について図8のフローチャートを用いて説明する。

【0052】まず、制御部131は、乱数生成部180に乱数を生成する指示を行う。乱数生成部180は、制御部131からの指示に基づいて、乱数Rを生成し(ステップS201)、生成した乱数Rを記憶部110に出力し、記憶部110に記憶する(ステップS202)。次に、制御部131は、分散部140に、秘密鍵SKを分割する指示を行う。分散部140は、制御部131からの指示に基づいて、秘密鍵SKを2つに分割し(ステップS203)、部分秘密鍵SKaと部分秘密鍵SKbとして記憶部110に記憶する(ステップS204)。

【0053】記憶部110に部分秘密鍵SKaが記憶された後、利用者によってICカード500がR/W170に挿入されると、制御部131は、記憶部110から部分秘密鍵SKaと乱数Rを読み出し、バス160とR/W170とを介してICカード500に転送する制御

を行う。ICカード500の通信部510は、R/Wから出力される部分秘密鍵SKaと乱数Rを受信すると、受信した部分秘密鍵SKaと乱数Rを記憶部530に記憶する(ステップS205)。

【0054】さらに、制御部131は、記憶部110から部分秘密鍵SKbと乱数Rとユニークコードf(i)を読み出し、部分秘密鍵演算部190に出力するとともに、部分秘密鍵SKbiを生成する指示をする。部分秘密鍵演算部190は、(1)式と、部分秘密鍵SKbと乱数Rとユニークコードf(i)に基づいて部分秘密鍵SKbiを生成し(ステップS205)、生成した部分秘密鍵SKbiを通信部150に出力し、店舗端末300に送信する指示をする。通信部150は、部分秘密鍵演算部190からの指示に基づき、ネットワーク400を介して店舗端末300に送信する(ステップS206)。店舗端末300の通信部370は、ネットワーク400を介して利用者端末100から受信した部分秘密鍵SKbiを受信し(ステップS207)、記憶部320に出力する。記憶部320は、通信部370から出力された部分秘密鍵SKbiを記憶する(ステップS208)。

【0055】次に、図7に戻り、ICカード500に部分秘密鍵SKaiが記憶され(ステップS)、店舗端末300に部分秘密鍵SKbiが記憶された後(ステップS103)、利用者は、ICカード500を携帯して、店舗端末300が設置されている店舗iへ出向き、従業員との間で取引に関する交渉を行う。そして、利用者と従業員との間で取引に関する交渉がなされた後、利用者が取引の契約をする場合、利用者によってICカード500がR/W390に挿入された後、利用者は、ユニークコードf(i)を店舗端末300の入力部310から入力する(ステップS103)。入力部310から入力されたユニークコードf(i)は、バス380とR/W390を介してICカード500に出力される。そして、ICカード500の通信部510入力によってユニークコードf(i)が受信され(ステップS104)、記憶部530に出力され、記憶される。

【0056】次に、店舗iの従業員からMsgの生成が指示されると、MSG生成部330によって署名対象となるMsgが生成され(ステップS105)、生成されたMsgが記憶部320に記憶されるとともに、R/W390を介してICカード500に送信される(ステップS106)。ICカード500の通信部510は、Msgを受信し(ステップS107)、Msgを記憶部530に出力し、記憶する。Msgが記憶部530に記憶されると、部分秘密鍵生成部550は、記憶部530に記憶されている部分秘密鍵SKaとユニークコードf(i)と乱数Rに基づいて、上記(2)式によって、部分秘密鍵SKaiを生成する(ステップS108)。そして、部分秘密鍵生成部550は、生成した部分秘密鍵

SKaiを記憶部530に記憶する。

【0057】部分秘密鍵SKaiが記憶部530に記憶されると、部分署名生成部520は、記憶部530に記憶された部分秘密鍵SKaiとMsgに基づいて、上記(3)式を用いて、部分署名Saを生成し(ステップS109)、記憶部530に記憶する。記憶部530に部分署名Saが記憶されると、通信部510は、記憶部530から部分署名Saを読み出して、R/W390を介して店舗端末300に送信する(ステップS110)。

【0058】一方、店舗端末300の部分署名生成部340は、部分秘密鍵SKbiとMsgを記憶部530から読み出して、上記(4)式を用いて、部分署名Sbを生成し(ステップS111)、記憶部530に記憶する。次に、R/W390を介してICカード500から部分署名Saを受信すると(ステップS112)、記憶部320は、部分署名Saを記憶する。部分署名Saが記憶部320に記憶されると、署名生成部350は、記憶部320に記憶された部分署名Saと部分署名Sbとを読み出して、上記(5)式を用いて署名Sを生成する(ステップS113)。署名Sが生成されると、署名Sが記憶部320に格納された後、署名検証部360によって、署名Sと利用者の公開鍵PKとが記憶部320を読み出され、署名Sが公開鍵PKによって検証される(ステップS114)。

【0059】なお、上述した第3の実施形態において、ユニークコードf(i)は、利用者だけが知り得る値であってもよく、店舗iが知り得る値であってもよい。また、ユニークコードf(i)は、すべての店舗iにおいて共通する値であってもよい。

【0060】次に、第4の実施形態について説明する。この実施形態においては、ユニークコードf(i)をMsgに設定する場合について図面を用いて説明する。図9は、第4の実施形態における電子署名システムの構成を示す概略ブロック図である。この図にいて、図6の各部に対応する部分には同一の符号を付け、その説明を省略する。この実施形態において、ユニークコードf(i)は、使用先コードIDiが設定される。この使用先コードIDiは、使用先の店舗iの固有の情報に基づいて決定される値であり、例えば、店舗iの名称のデータが用いられる。

【0061】次に、部分秘密鍵演算部190は、部分秘密鍵SKbと乱数Rとf(i)とに基づいて、上述の(1)式を用いて部分秘密鍵SKbiを演算するが、この実施形態において、ユニークコードf(i)が使用先コードIDiとなるので、以下に示す(6)に基づいて、部分秘密鍵SKbiを演算する。

$$SKb + H(IDi \parallel R) \cdots \cdots (6)$$

【0062】ICカード500の部分秘密鍵演算部550は、部分秘密鍵SKaと乱数Rとユニークコードf(i)とに基づいて、上述の(2)式を用いて部分秘密

鍵SK*a i*を演算するが、この実施形態において、ユニークコード*f(i)*が使用先コードID*i*となるので、以下に示す(7)に基づいて、部分秘密鍵SK*a i*を演算する。

$$SKa = H(IDi \parallel R) \quad \cdots \cdots (7)$$

【0063】部分署名生成部521は、部分署名生成部520の機能においてさらに、記憶部530から使用先コードID*i*を読み出し、Msgに使用先コードID*i*を付加して部分署名Saを生成する。この部分署名生成部521は、以下に示す(8)式に基づいて部分署名Saを生成する。

$$Sa = IDi \cdot MSG^{SKai} \bmod(n) \quad \cdots \cdots (8)$$

部分署名生成部341は、部分署名生成部340の機能においてさらに、記憶部320から使用先コードID*i*を読み出し、Msgに使用先コードID*i*を付加して部分署名Sbを生成する。この部分署名生成部341は、以下に示す(9)式に基づいて部分署名Sbを生成する。

$$Sb = IDi \cdot MSG^{SKbi} \bmod(n) \quad \cdots \cdots (9)$$

このような構成において、装置の各部は、図7と図8における説明と同様に動作する。このように、Msgに使用先コードID*i*を付加して部分署名Sa、部分署名Sbが生成され、この部分署名Saと部分署名Sbとに基づいて、署名生成部350によって署名Sが生成されると、図10符号600に示すように、使用先コードID*i*に関する情報がMsg(符号610)内に設定される。これにより、利用者は、部分秘密鍵SK*b i*の送信となる店舗*i*でしか生成できないMsgに対して電子署名を行うことが可能である。従って、第三者によって電子署名(符号630)が設定された契約書内の契約先の名称(符号620)が、利用者が実際には契約を行っていない場合の契約先の名称に改竄された場合、改竄された契約先名称とMsgに予め設定されている契約先の名称(符号600)とが異なるので、改竄を発見することが可能であり、署名Sを部分秘密鍵SK*b i*の預け先以外に流用されることを防ぐことが可能である。

【0064】なお、上述した第3の実施形態と第4の実施形態において、ユニークコード*f(i)*は、店舗端末300に部分秘密鍵SK*b*を送信するときに同時に送信するようにしてもよい。

【0065】次に、第5の実施形態について図面を用いて説明する。図11は、第5の実施形態における電子署名システムの構成について説明するための概略ブロック図である。この実施形態では、しきい値*k*を3に設定して、部分秘密鍵を利用者端末100とICカード500と店舗端末300に設定する場合を一例として説明する。図11において、図9の各部に対応する部分には同一の符号を付け、その説明を省略する。部分署名生成部195は、記憶部110から使用先コードID*i*を読み出し、Msgに使用先コードID*i*を付加して部分署名

Scを生成する。この部分署名生成部195は、以下に示す(10)式に基づいて部分署名Scを生成する。

$$Sc = IDi \cdot MSG^{SKci} \bmod(n) \quad \cdots \cdots (10)$$

【0066】次に、図11の構成における装置の動作について、図面を用いて説明する。図12は、図11の構成における装置の動作について説明するためのフローチャートである。まず、図1のステップS1の処理と同様に、利用者端末100によって公開鍵PKが認証機関端末200に登録され、秘密鍵SKが記憶部110に記憶されるとともに、店舗端末300によって、認証機関200から利用者の公開鍵PKが読み出され、記憶部320に記憶される。また、従業員によって設定される使用先コードID*i*が記憶部320に記憶される。次に、利用者は、入力部120から、入力部120から秘密鍵SKの分割が指示されると、制御部130は、記憶部110から秘密鍵SKを読み出して分散部140へ出力するとともに、しきい値3で3個に分割する指示を行う。さらに、制御部131は、乱数生成部180に乱数の生成を指示する。

【0067】分散部140は、制御部131からの指示を受けて、秘密鍵SKを3つに分割し、部分秘密鍵SK*a*、部分秘密鍵SK*b*、部分秘密鍵SK*c*を生成する(ステップS301)。そして、分散部140は、生成した部分秘密鍵SK*a*、部分秘密鍵SK*b*、部分秘密鍵SK*c*を記憶部110に記憶する(ステップS302)。

【0068】一方、乱数生成部180は、制御部131からの指示に基づいて、乱数Rを生成し、記憶部110に記憶する。次に、制御部131は、記憶部110に記憶された部分秘密鍵SK*a*と乱数Rを読み出し、R/W170を介してICカード500に送信する(ステップS303)。ICカード500の通信部510は、利用者端末100から送信された部分秘密鍵SK*a*と乱数Rを受信し、記憶部530に記憶する(ステップS304)。

【0069】次に、制御部131は、記憶部110から部分秘密鍵SK*b*と乱数RとID*i*を読み出して、部分秘密鍵演算部190に出力するとともに、部分秘密鍵SK*b i*を生成する指示をする。部分秘密鍵演算部190は、制御部131からの指示に基づいて、部分秘密鍵SK*b i*を生成し、記憶部110に記憶した後、通信部150とネットワーク400を介して、店舗端末300に送信する(ステップS305)。店舗端末300の通信部370は、部分秘密鍵SK*b i*を受信すると、記憶部320に記憶する(ステップS306)。

【0070】次に、利用者は、ICカード500を携帯するとともに、利用者端末100をネットワーク400を介して通信可能な状態に設定しておき、店舗*i*に出向く。そして、利用者は、従業員と交渉を行い、契約を行う場合、従業員に契約書となるMsgの生成を依頼す

る。従業員は、店舗端末300によってMsg生成し、生成されるMsgと使用先コードID iとを利用者端末100に送信する指示を行う。

【0071】店舗端末300のMSG生成部330は、入力部120から入力される従業員からの指示に応じて、Msgを生成し、生成したMsgを記憶部320に記憶するとともに、通信部370とネットワーク400を介して利用者端末100に送信する。このとき、入力部310から入力される使用先コードID iの送信指示に応じて、記憶部320から使用先コードID iが読み出され、上記Msgと同様に、利用者端末100に送信される(ステップS308)。

【0072】次に、店舗端末300からMsgと使用先コードID iが送信されると、通信部150は、Msgと使用先コードID iを受信して記憶部110に記憶する(ステップS309)。Msgと使用先コードID iが記憶部110に記憶されると、部分署名生成部195は、記憶部110からMsg、部分秘密鍵SK c、使用先コードID iを読み出し、これらに基づいて、使用先コードID iをMsgに付加して部分署名Scを生成する。生成された部分署名Scは、通信部150によって、ネットワーク400を介して店舗端末300に送信される(ステップS311)。

【0073】店舗端末300において、通信部370は、部分署名Scを受信すると、記憶部320に記憶する(ステップS312)。そして、利用者によってICカード500がR/W390に挿入されると、記憶部320に記憶されているMsgと使用先コードID iが読み出され、ICカード500に送信される(ステップS313)。ICカード500の通信部510は、受信したMsgと使用先コードID iを記憶部530に出力して記憶する(ステップS314)。Msgと使用先コードID iが記憶されると、部分秘密鍵生成部550は、部分秘密鍵SK aと乱数Rと使用先コードID iとに基づいて、部分秘密鍵SK a iを生成し(ステップS315)、記憶部530に記憶する。部分秘密鍵SK a iが生成されると、部分署名生成部521は、Msgに使用先コードID iを付加して部分秘密鍵SK a iを用いて部分署名Saを生成し(ステップS316)、通信部510とR/W390を介して店舗端末300に送信するとともに(ステップS317)、記憶部530に記憶する。

【0074】店舗端末300において部分署名Saを受信すると(ステップS318)、受信した部分署名Saを記憶部320に記憶する。部分署名Saを受信した後、部分署名生成部341は、部分秘密鍵SK b iと乱数Rと使用先コードID iを記憶部320から読みだし、部分署名Sbを生成する(ステップS319)。部分署名Sbが生成されると、署名生成部350は、部分署名Sa、Sb、Scから署名Sを生成し(ステップS

320)、生成した署名Sを記憶部320に記憶する。署名検証部360は、記憶部320から利用者の公開鍵PKを読み出し、公開鍵PKによって生成された署名Sを検証する(ステップS321)。

【0075】なお、第5の実施形態において、秘密鍵SK、部分秘密鍵SK a、部分秘密鍵SK b、部分秘密鍵SK c、乱数Rを利用者端末100、ICカード500以外の記録媒体に記録し、バックアップ用として保管してもよい。

【0076】また、上記実施形態において、利用者端末100にアクセスがある毎にログにアクセスの履歴を記憶するようにしてもよい。これにより、利用者がICカードを紛失したり、ICカードの部分秘密鍵がコピーされ、拾得者や悪意ある第3者がICカードを不正使用しようとした場合においても利用者端末100にアクセスの履歴が記録される。従って、利用者ICカードの所有者である利用者は、不正使用されることを把握でき、利用者端末100を停止させることによって、以後の不正使用を防止することが可能である。また、利用者端末100に記録されたアクセス履歴を参照することにより利用者は、不正使用された状況を把握することが可能である。このように、自宅の利用者端末100にも部分秘密鍵SK cを保管することにより、利用者は、部分秘密鍵の不正使用の検出、不正使用された状況の把握をすることが可能である。

【0077】また、上記実施形態において、利用者端末100における通信部110に利用者が携帯する携帯電話へ通信する機能を設け、利用者端末100にアクセスがある毎に携帯電話に発信または、電子メールを利用者に送信するようにしてもよい。これにより、利用者は、利用者端末100へのアクセス状況を把握できるので、予期しないアクセスをより早期に発見することが可能である。

【0078】また、上記実施形態において、利用者端末100に部分秘密鍵を保管し、アクセスするようにしたが、利用者の部分秘密鍵を保管する共同センタ端末を設け、この共同センタ端末に部分秘密鍵を保管し、店舗端末300からのアクセスを受けるようにしてもよい。

【0079】また、上記実施形態において、利用者端末100にパスワードを設定し、店舗端末300からのアクセス時において、入力されるパスワードが一致しない場合に、利用者端末100にアクセスできないようにしてもよい。これにより、利用者端末100に不正にアクセスすることを防止することができる。

【0080】次に、部分秘密鍵の更新について図11の構成における電子署名システムを例として図13を用いて説明する。図13は、部分秘密鍵の更新を行う動作について説明するためのフローチャートである。まず、利用者端末100において、制御部131は、部分秘密鍵SK aと部分秘密鍵SK cとを記憶部110から読み出

し(ステップS401)、一時保持する。次に、制御部131は、乱数生成部180によって乱数aを生成させ、生成された乱数aを取得し、一時保持する(ステップS402)。次に、制御部131は、以下に示す(11)式と(12)式に基づいて、新たな部分秘密鍵SKa'、部分秘密鍵SKc'を生成する。

$$SKa' = SKa + a \dots\dots (11)$$

$$SKc' = SKc - a \dots\dots (12)$$

制御部131は、生成された部分秘密鍵SKa'と部分秘密鍵SKc'とを記憶部110に記憶するとともに、部分秘密鍵SKa'をICカード500の記憶部530に記憶する制御を行う。これにより、利用者端末100の部分秘密鍵SKa'、ICカード500の部分秘密鍵SKc'を更新することができる。

【0081】上述した、ICカードと利用者端末100の部分秘密鍵の更新を行うことによって、ICカードの紛失、盗難が発生した場合や、ICカードの部分秘密鍵がコピーなどによってデータが持ち出された場合においても、ICカードの部分秘密鍵を無効にすることができるので、ICカードの停止をすることが可能である。また、利用者端末100において部分秘密鍵の更新を行うことができるので、公開鍵明書を再取得したり、店舗に部分秘密鍵を再登録する手間を省くことができる。

【0082】また、図1における処理部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより施工管理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境(あるいは表示環境)も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー(登録商標)ディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

### 【0083】

【発明の効果】以上説明したように、この発明によれば、電子署名を生成するための鍵情報を分割し、ICカードと店舗端末に記憶するようにしたので、分割した部分鍵情報を有しない店舗においては、電子署名を生成することができないので、ICカードの使用できる店舗を限定でき、秘密鍵の紛失、盗難、盗聴などが発生した場合においても、悪意ある第三者によって秘密鍵が悪用される可能性を低減させることができ、鍵情報の機密性を向上できる効果が得られる。

【0084】また、この発明によれば、鍵情報を分割して部分鍵情報を生成し、一度分割した部分鍵情報をさらに分割して各店舗端末に送信し、一度分割された部分鍵情報と二度分割された部分鍵情報の一部とをICカードに記憶するようにしたので、使用先となる店舗同士が結託し、部分鍵情報を用いて署名を作成する、部分鍵情報を流用するといった使用先の不正使用を防止することができる効果が得られる。

【0085】また、この発明によれば、メッセージに使用先コードを付加して部分署名を生成し、これらの部分署名を集めて電子署名を生成するようにしたので、ICカードの利用者は、部分鍵情報の送信となる店舗でしか生成できないメッセージに対して電子署名を行うことが可能である。従って、第三者によって電子署名が設定されたメッセージの契約書内の契約先の名称が、利用者が実際には契約を行っていない場合の契約先の名称に改竄された場合、改竄された契約先名称とメッセージに予め設定されている契約先の名称とが異なるので、改竄を発見することが可能であり、電子署名を部分鍵情報の預け先以外に流用されることを防ぐことが可能である。

### 【図面の簡単な説明】

【図1】 この発明の一実施形態による電子署名システムの構成を示す概略ブロック図である。

【図2】 シークレットシェアを説明するための概念図である。

【図3】 図1の構成における電子署名システムの動作について説明するためのフローチャートである。

【図4】 第2の実施形態における電子署名システムの構成を示す概略ブロック図である。

【図5】 図4の構成における電子署名システムの動作について説明するためのフローチャートである。

【図6】 第3の実施形態における電子署名システムの構成を示す概略ブロック図である。

【図7】 図6の構成における装置の動作について説明するためのフローチャートである。

【図8】 部分秘密鍵SKa、部分秘密鍵SKbiをICカード500、店舗端末300に設定する動作を説明するためのフローチャートである。

【図9】 第4の実施形態における電子署名システムの構成を示す概略ブロック図である。

【図10】 使用先コードIDiがMsg内に設定された状態を説明するための概念図である。

【図11】 第5の実施形態における電子署名システムの構成について説明するための概略ブロック図である。

【図12】 図11の構成における装置の動作について説明するためのフローチャートである。

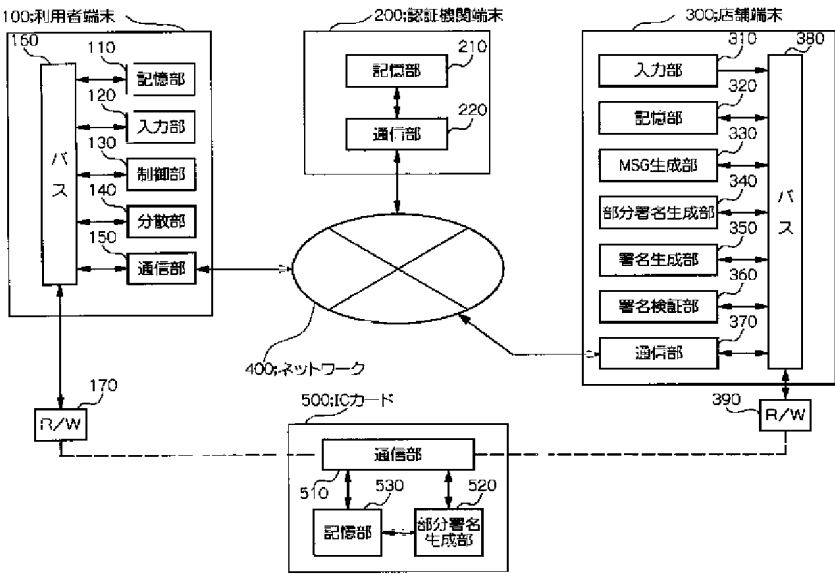
【図13】 部分秘密鍵の更新を行う動作について説明するためのフローチャートである。

【符号の説明】

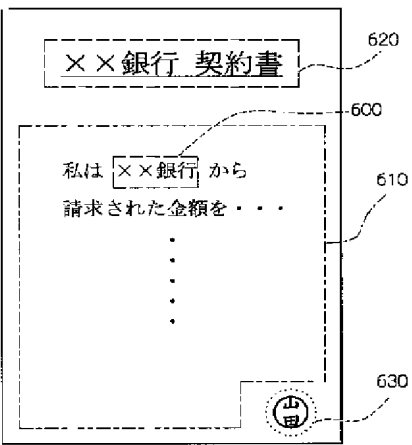
100 利用者端末、 110 記憶部、 130 制御部、 140 分散部、 150 通信部、 170 R/W、 200 認証機関端末、 210 記憶部、 220 通信部、 300 店舗端末、 310 入力部、 320 記憶部、 330 MSG生成部、 340 部分署名生成部、 350 署名生成部、 360 署名検証部、 370 通信部、 390 R/W、 500 ICカード、 510 記憶部、 520 部分署名生成部、 530 通信部、 600 契約書、 610 署名、 620 銀行名、 630 印

0、131 制御部、140、141 分散部、 150 通信部、 180 乱数生成部、190 部分秘密鍵演算部、 195 部分署名生成部、300 店舗端末、 320 記憶部、 330 MSG生成部、340、341 部分署名生成部、 350、351 署名生成部、370 通信部、 500 ICカード、520、521 部分署名生成部、 530 記憶部、540 署名生成部、 550 部分秘密鍵生成部

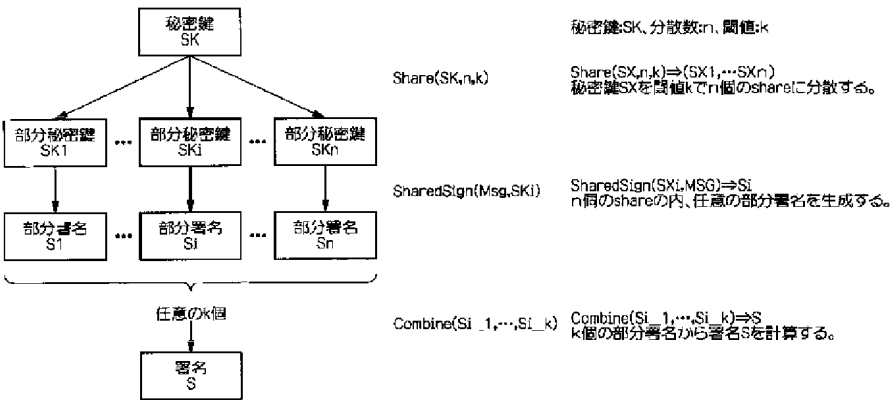
【図1】



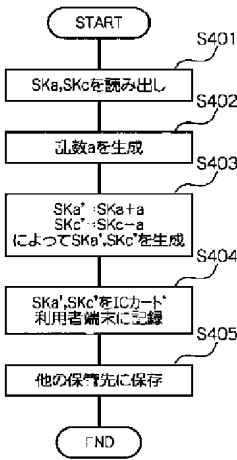
【図10】



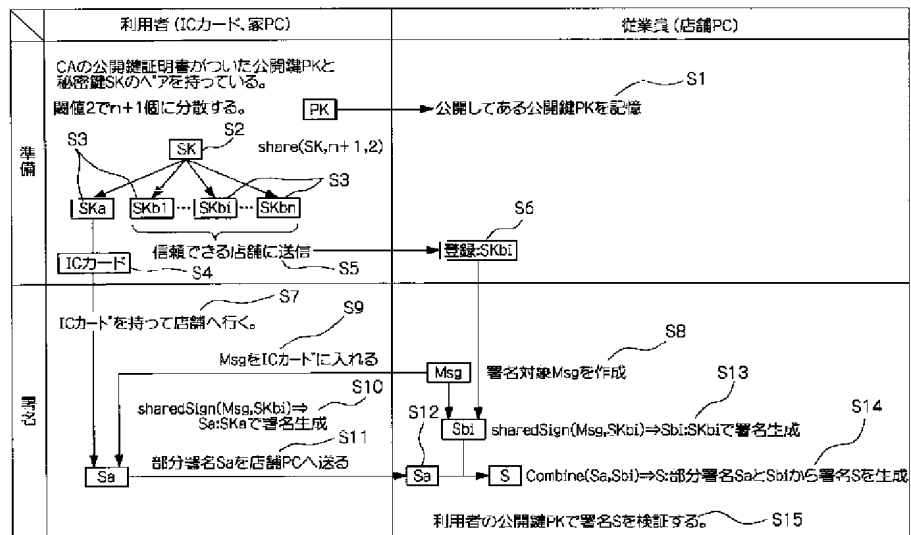
【図2】



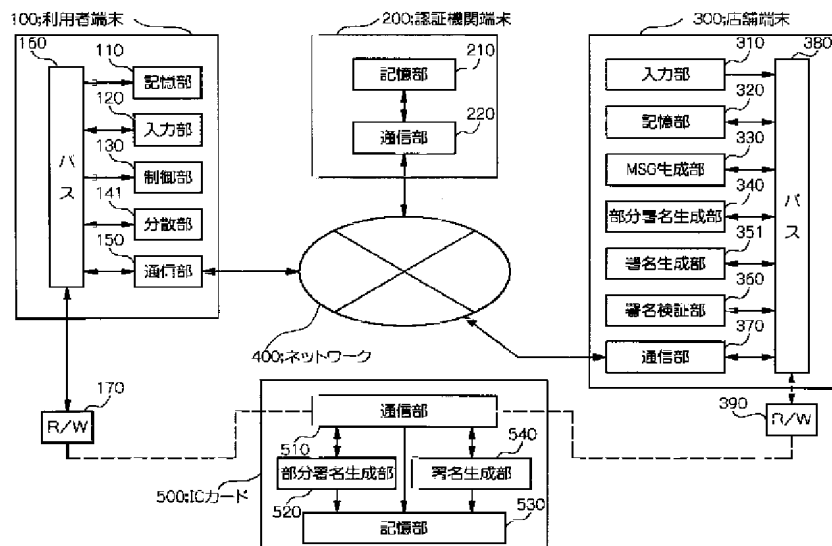
【図13】



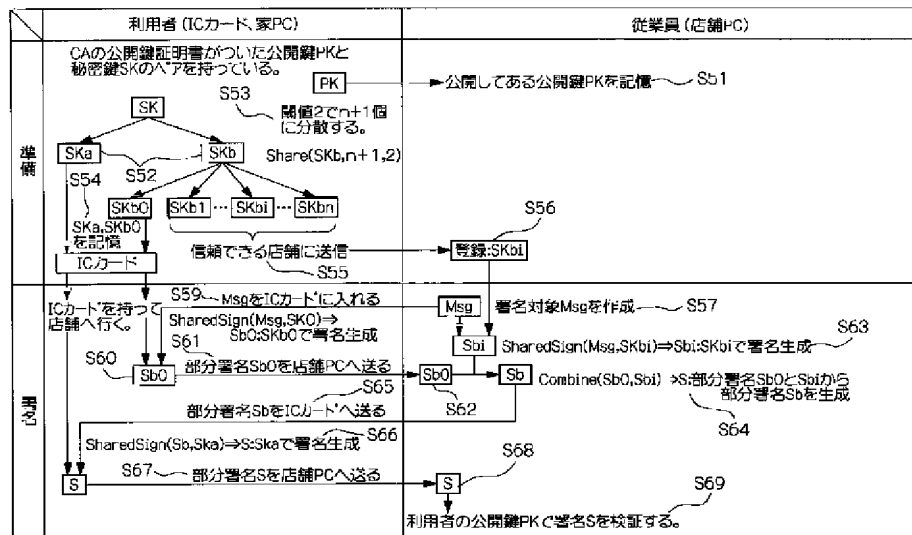
【図3】



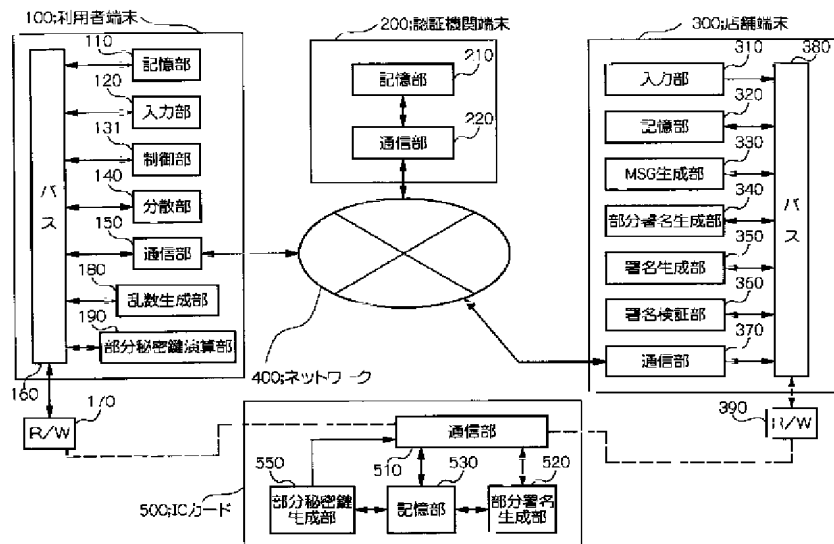
【図4】



【図5】

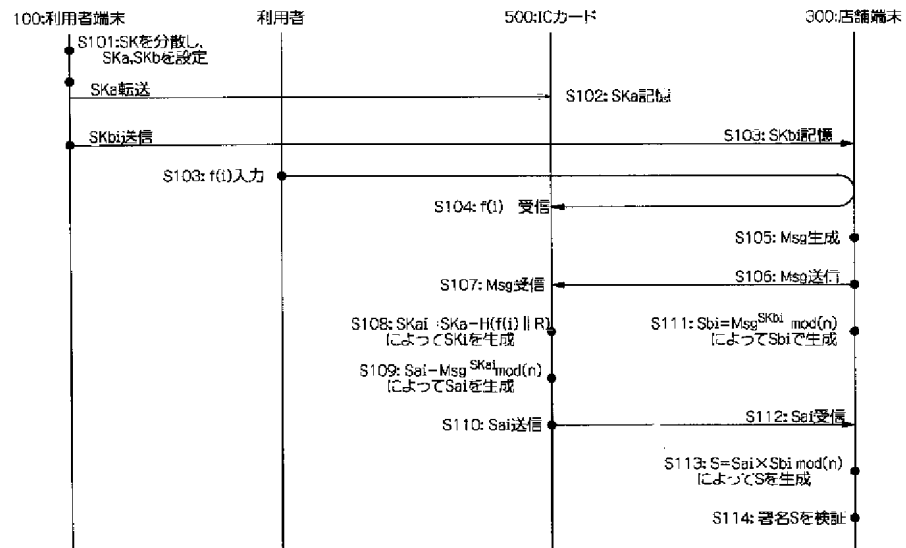


【図6】

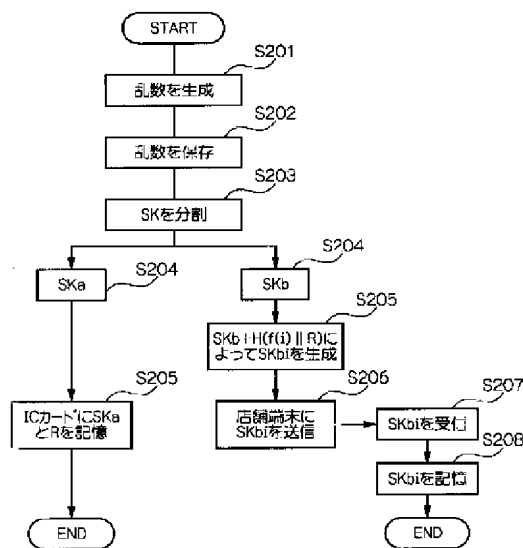




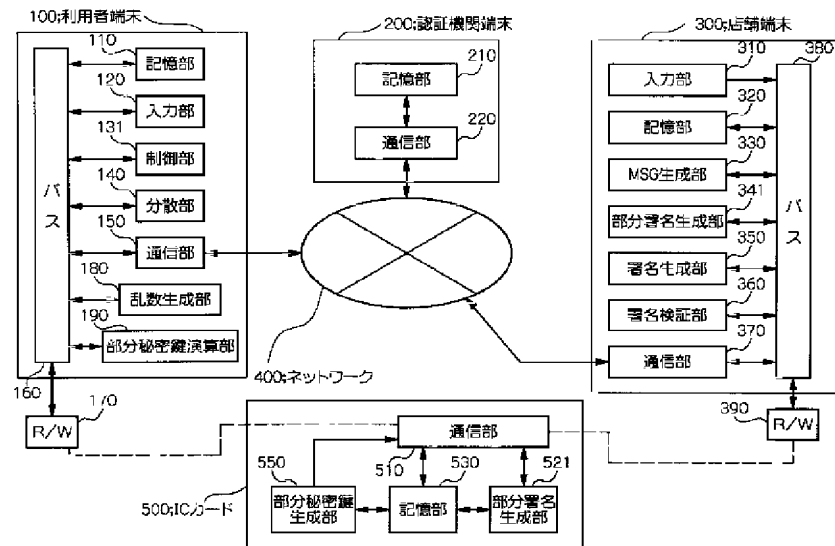
【図7】



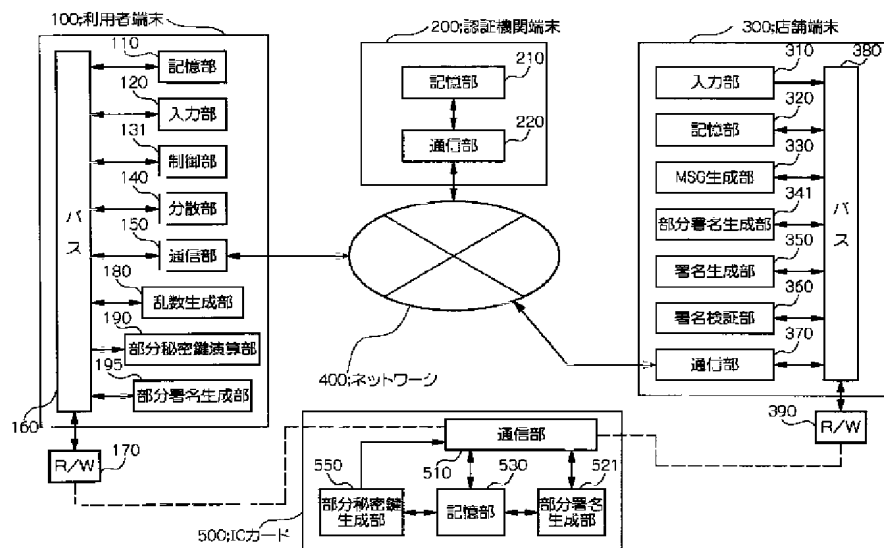
【図8】



【図9】



【図11】



【図12】

